PCI Compliance Guidelines for Delphi's Endura™ 15X Order Confirmation System

Introduction

The PCI DSS (Payment Card Industry Data Security Standard) is a set of security requirements that helps businesses protect their payment systems from breaches, fraud and theft of cardholder data. The standard is developed and maintained by the PCI Security Standards Council, which is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. On December 15, 2004, PCI DSS Version 1.0 was released and has evolved over the past 15 years where as of January 1, 2019, all merchants are required to comply with PCI DSS version 3.2.1. In this paper, we provide an overview of the inherent security features built into Delphi's Endura™ 15X Drive Thru Order Confirmation System as well as general implementation guidelines that will ensure PCI DSS compliance within the installation site IT infrastructure.

Terminology

The following terms and acronyms are used throughout this paper:

- CDE – Cardholder data environment
- CHD – Cardholder data
- SAD – Sensitive authentication data
- Account Data – Cardholder data and/or sensitive authentication data
- OCS – Order Confirmation System

PCI DSS Compliance Overview

The PCI DSS applies to ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. There are twelve basic requirements of PCI compliance listed below.

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Out of Scope Requirements

A system is considered to be out of the scope of PCI compliance if it meets the following requirements.

- System does not store, process, or transmit CHD or SAD
- AND System is NOT in the same network segment as systems that store, process or transmit SAD or CHD

- AND System cannot connect to any system in the CDE
- AND System does NOT meet any criteria described for connected-to or security-impacting systems:
    - Directly or indirectly connect to CDE
    - Impacts configuration or security of CDE
    - Provides security services to the CDE
    - Segments CED systems from out of scope systems and networks
    - Supports PCI DSS requirements

PCI DSS Compliance Guidelines

For each of the twelve requirements of PCI compliance, we will make recommendations on best practices on how to meet the requirement when utilizing the Endura 15X Order Confirmation System within your IT environment.

1. Install and maintain a firewall configuration to protect cardholder data.

One of the most effective means of protecting cardholder data is to segment the network using either firewalls or physical separation to restrict CHD to only the devices and network that processes CHD. Network segmentation is the most common and effective means to accomplish this.

Network segmentation is the process of sectioning off one network into smaller segments, or "subnetworks," in such a way that limits or prevents communication between them. It's a key security practice for any merchant that wants to protect their cardholder data and reduce their PCI scope. Reducing PCI scope in itself will save time, money, and effort. When done properly, network segmentation provides controls that limit or stop communication from one subnetwork into another. When done improperly—or not thoroughly enough—hackers may be able to "pivot" from a less-secure area (such as an office zone) into your cardholder data environment (CDE).

The Target Data Breach of 2013 was possible thanks to a basic network segmentation error. Hackers started by using stolen credentials to log in to a 3rd-party vendor's application, which was running in a non-CDE area of Target's network. This area was not properly segmented. The attackers then performed a "pivot attack" and moved into Target's CDE. From there, they installed malware and siphoned around 40 million credit card numbers from point-of-sale devices. Therefore, it is critical to understand how to properly segment the network to prevent these pivot attacks.

The most common way to segment is by implementing a piece of dedicated hardware that sits between network zones to limit network traffic, also known as a firewall. The most important part of firewall implementation is configuring the Access Control List (ACL) to define exactly what traffic can pass. Proper firewall configuration will limit communication to the OCS to only the real time POS transaction data and prevent any CHD on the OCS network segment. This configuration should restrict connections between untrusted networks and any system components in the CDE and prohibit direct public access between the Internet and any system component in the CDE.

2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Delphi configures custom system passwords and other security parameters on each OCS prior to shipment to the customer, however, as with all equipment on the network, it is highly recommended that the customer changes all passwords and login credentials from their default values prior to installing and configuring on the network. Configuration standards should be developed for all system components and assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

By establishing and maintaining robust organizational security standards and policies that ensure adherence to processes for resetting passwords, keeping current on requirements, and establishing clear internal standards to follow, can mitigate the threat of fraudulent password access to data.

3. Protect stored cardholder data.

In order to protect card holder data, it is necessary to keep cardholder data storage to a minimum, retain only what is absolutely necessary to meet regulatory, legal or business requirements and securely delete what's not necessary. The OCS does not process or store any CHD at any time.

4. Encrypt transmission of cardholder data across open, public networks.

Strong cryptography and security protocols are essential for safeguarding CHD when it is being transmitted over open, public networks. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. Websites that accepts card holder payments must use TLS v1.1 and higher as a mandatory requirement for PCI compliance. The OCS uses self-signed certificates and HTTPS encrypted protocols for the management of system configuration and content. All passwords are encrypted and stored in the local database. The OCS does not process, store or transmit any CHD over the its network connection.

5. Use and regularly update anti-virus software.

In order to comply with this requirement, we recommend that antivirus and anti-malware software be deployed on all connected equipment on the network that could be vulnerable to these types of attacks. It is imperative to ensure that all antivirus mechanisms are maintained and are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. All related security policies and procedures should be documented and maintained.

6. Develop and maintain secure systems and applications.

To comply with this requirement, it is critical to keep all software and security patches current to protect your network and the CDE. Where it is impractical to update and maintain software patches on some systems, firewalls that offer virtual patching can help prevent the exploitation of known vulnerabilities. While the OCS does not typically have direct access to the internet for providing software updates, patching systems can be implemented on the OCS network segment to allow the operating system to be patched as required.

7. Restrict access to cardholder data by business need-to-know.

Access to the CDE should be limited to only those individuals whose job requires such access. All security policies and procedures should be documented and kept current. This requirement does not apply to the OCS since it does not process, store or transmit any CHD.

8. Assign a unique ID to each person with computer access.

In order to comply with this requirement, it is necessary to create and document policies and procedures to ensure only specific individuals have access to CHD. This can be done by assigning unique and secure IDs and implementing two-factor authentication for both employees and third-party vendors. Avoid using group, shared, or generic IDs, passwords, or other similar authentication methods and restrict access to any database containing CHD. Again, it is important to document and maintain all of these policies and procedures. This requirement does not apply to the OCS.

9. Restrict physical access to cardholder data.

To restrict physical access to cardholder data, several measures can be taken. First, by restricting access to network connections will prevent unauthorized users from potentially accessing the CDE. Proper installation of the OCS requires it to be in a locked enclosure to prevent unauthorized access to its network connection. Further segmentation of the network as described in requirement #1 above will prevent access to CHD even if the physical network connection is compromised. Second, it is important to restrict access to network equipment by only those authorized to do so. Lastly, make sure all copies of CHD are secured or deleted if not needed.

10. Track and monitor all access to network resources and cardholder data.

This requirement states that audit trails and review logs must be implemented to monitor access to network assets and identify a compromise or data breach. Failure to properly log all internal and external users may limit your ability to pinpoint a breach timeline or identify who is responsible for a compromise. Additional measures such as integrity monitoring systems should be implemented to verify and alert of any suspicious changes to DNS settings, SSL certificates, or modifications of core files. This requirement relates to the network administration and policies and does not apply directly to the OCS.

11. Regularly test security systems and processes.

To comply with this requirement, it is good practice to run vulnerability scans and penetration testing regularly and after any significant changes to the network. Any changes to system, configuration, or content files should be monitored and checked. Effective 1 February, 2018, service providers must perform penetration testing at least every six months to verify segmentation controls. As with any of these procedures, everything should be documented and maintained. This requirement relates to the network administration and policies and does not apply directly to the OCS.

12. Maintain a policy that addresses information security.

This requirement contains several sub-requirements including the establishment of an information security policy, implementation of a risk-assessment process with assigned security responsibilities, development of usage policies for critical technologies, insurance that the security policies and procedures clearly define expectations and responsibilities of any persons with access including awareness of the importance of protecting customer data, implementation of new employee and any third-party service provider screening policies for individuals with access to cardholder data to minimize the risk of attacks from internal sources and the implementation of an incident response plan to ensure immediate response to a system breach.

Additional Information on the inherent security built into the Endura 15X OCS

In designing the architecture of the Endura 15X Order Confirmation System, Delphi has taken several steps to improve the security of the system including:

1. All network connections are initiated as outbound.
2. All APIs use self-signed certificates and HTTPS encrypted communications.
3. All data is encrypted in place and in transit.
4. The OCS only opens a limited number of network ports for communication to the Point of Sale and Back of House systems including ports 21, 22, 80, 443, 8080, 8443, 48501 and 48502.
5. The Endura 15X OCS utilizes Linux Ubuntu operating system which is inherently more secure and less vulnerable than Windows and allows the system to be customized to meet specific customer security requirements.

Conclusion

The Payment Card Industry Data Security Standard is focused on minimizing the risk of sensitive payment card holder information being compromised. Delphi's Endura 15X Order Confirmation System was designed with PCI Compliance in mind and is the most secure network product of its kind on the market today. By paying special attention to the twelve PCI compliance requirements, leveraging industry best practices and utilizing PCI compliant equipment, the risk of a card holder data security breach is greatly reduced.

For additional information, please contact Delphi Display Systems at DelphiDisplay.com or visit the PCI Security Standards Council web site at https://www.pcisecuritystandards.org.